WHALLEY PARISH COUNCIL

This document sets out the Parish Council's

Information Technology Policy

Version Control

Version	Date	Description of Change
V.1	15/5/2025	New Policy

WPC Parish Council IT Policy

1. Purpose
This policy outlines the proper use of IT equipment, systems, and software by members, the Clerk, and any other staff or contractors of the Parish Council. It ensures that all business is conducted securely, legally, and in line with best practices for data protection and public service accountability.

2. Scope
This policy applies to:

- All Parish Council members
- The Clerk
- Council employees, contractors, and volunteers
- Use of both Council-owned and personal devices when conducting Council business

3. Principles of Use
All individuals must:

- Use IT resources responsibly and ethically
- Protect Council data and systems from unauthorised access or disclosure
- Ensure compliance with legal and regulatory obligations, including the Data Protection Act 2018 and UK GDPR
- Maintain transparency and accountability in all communications and document handling

4. Acceptable Use

4.1 Council-Owned Devices and Software

- Must be used only for Council business
- Software must be licensed and approved by the Council
- Users must not install unauthorised applications
- Devices should be secured with passwords and kept updated

4.2 Personal Devices

- May be used for Council business only if approved by the Council
- Must have suitable security features (e.g., passwords, antivirus software, encrypted storage)

- Users must ensure Council data is not stored insecurely or shared inappropriately
- Loss or theft of any personal device used for Council business must be reported immediately

5. Email and Communication

- Council-provided email addresses must be used for all Council correspondence
- Personal email accounts must not be used to conduct Council business
- Users must not share sensitive information via unsecured platforms

6. Data Protection and Confidentiality

- All users must handle personal data in accordance with data protection laws
- Confidential information must not be disclosed without appropriate authority
- Documents must be stored securely, whether digitally or physically

7. Cloud Services and Document Sharing

- Only Council-approved cloud storage (e.g., Microsoft OneDrive, Google Workspace) may be used
- Documents must not be stored or shared via personal cloud accounts
- Access permissions must be managed to ensure confidentiality and version control

8. Cybersecurity Requirements

- Devices must have up-to-date antivirus and firewall software
- Users must complete periodic cybersecurity awareness training (as provided by the Clerk or Council)
- Passwords must be strong and changed regularly
- Users must not share login credentials

9. Remote Working

- Must comply with all elements of this policy
- Public Wi-Fi should be avoided unless using a VPN
- Documents and devices must not be left unattended in public areas

10. Breaches and Enforcement

- Any suspected breach of this policy must be reported to the Clerk immediately
- Breaches may result in disciplinary action or referral to the Monitoring Officer
- Significant data breaches must be reported to the Information Commissioner's Office (ICO) if required

11. Policy Review

This policy will be reviewed annually or following any major changes in law or IT systems.